State of Vermont

User Password Policy

and Guidelines

Contents

1.0 Introduction....3

1.1 Authority....3

1.2 Purpose....3

1.3 Scope....3

2.0 Policy....3

2.1 General....4

2.2 Password Construction....4

2.3 Password Change....5

2.4 Password Reuse....5

3.0 Password Protection....5

3.1 Training....6

3.2 Enforcement....6

4.0 Exceptions....6

Appendix A: General Password Construction and Guidelines....7

1.0 Introduction

1.1 Authority

VSA 22 § 901 (1), authorizes the Department of Information and Innovation "to provide direction and oversight for all activities directly related to information technology and security in state government."

1.2 Purpose

Passwords are an important component of information technology and network security. The use of a password in combination with the user name serves to identify those who are authorized to have access to system resources and information assets. Authenticated access is one way that the enterprise can be assured that systems and data are being used appropriately. As such, passwords must be constructed, used, changed on a regular basis and protected appropriately to ensure that the level of security they imply is actually met.

The purpose of this policy is to provide the guidelines necessary for all of the employees of the State of Vermont as well as state partners, vendors, contractors with accounts, to create appropriate passwords and to use them and protect them in an appropriate manner.

1.3 Scope

This is one of two policies that will address passwords.

The scope of this policy applies to all persons who have or are responsible for an account (or any form of access that supports or requires a password) on any system that resides on any State of Vermont computer or network that requires a user name and password. ***The scope of this policy applies to the users of the states networks.***

The second policy will address accounts and passwords used by IT professionals for the administration of systems.

2.0 Policy

Passwords are the foundation of virtually all access and user management security systems. Passwords typically allow access to the data managed and controlled by departments and agencies. The complexity, use and management of passwords should reflect the classification of the data that is being protected or accessed. There may be instances where two factor authentication or biometrics may be required to access

specific accounts. If that is the case, this should be reflected in a specific agency or department written procedure.

2.1 General

For the purpose of this policy all passwords will be "strong" passwords. A "strong" password is defined as follows:

> Be a minimum of eight (8) characters in length, must use at least one character of three of the four character types, those being: lower case letters, upper case letters, numbers and special characters (Example: !, #, %). An example of a strong password is: *paSSw0rd!* It contains lower case and upper case letters, contains a number (0), has a special character (!) and is nine characters long. *Note: DO NOT use this as a password!*

Passwords will not be based on data classification to accommodate ease of administering the passwords.

1. Passwords should not be based on well-known or easily accessible information, including personal information. They should not be words commonly found within a standard dictionary.
2. Users will be notified two weeks in advance of password expiration. At that point, and at every subsequent login until a change is made, users will be prompted to select a new password. If a new password is not entered, the users account will automatically be locked. The user will need to notify their IT department to regain access to their account and change their password.
3. Passwords must not be inserted into e-mail messages or other forms of electronic communication.
4. The State of Vermont IT departments will use technical measures (rule settings within the application) to ensure that users conform to this policy.

2.2 Password Construction

See Appendix A at the end of this document, **General Password Construction Guidelines**, for more detailed information on password construction and guidelines.

Agency/department IT staff will be responsible for administering the technical requirements for user passwords settings.

Account holders are responsible for resetting their passwords.

2.3 Password Change

1. Passwords must be changed every ninety (90) days, at minimum, to reduce the risk of compromise through guessing, password cracking or other attack and penetration methods. *Exception: If a user terminates for any reason, passwords and accounts should be disabled immediately by the appropriate IT department personnel.*
2. Password changes shall be systematically enforced where possible.
3. Passwords shall be systematically disabled after ninety days of inactivity to reduce the risk of compromise.

2.4 Password Reuse

1. Passwords used to access data classified as "Confidential" may be reused every sixth password. As such a completely new password is required for the first five expires; thereafter, the first password can be reused. "Completely new" is defined as having at least fifty percent (50%) of the characters different from the previous password.

3.0 Password Protection

For passwords to be effective there are general guidelines that have to be adhered to. These guidelines are listed below.

1. Passwords are to be treated as confidential information. Under no circumstances is an employee to give, tell, or hint at their password to another person, including IT staff, administrators, superiors, other co-workers, friends and family members.
2. Under no circumstances will any member of the organization request a user's password without that request coming from both a representative of the IT department and the user's direct manager. Should a request be made that does not conform to this policy, the employee should immediately inform both the IT department and their direct manager.
3. Agencies/departments and users shall not transmit passwords electronically over the unprotected Internet, such as via e-mail.
4. Do not use the "Remember Password" feature of applications (e.g., Outlook, websites, organizational sites.)
5. User account lockout feature shall disable the user account after three (3) unsuccessful login attempts.
6. Account lockout duration shall be permanent until an authorized system administrator reinstates the user account.

7. No employee is to keep an unsecured written record of passwords, either on paper or in an electronic file unless kept in a controlled access safe or an encrypted file.
8. If an employee either knows or suspects that his/her password has been compromised, it must be changed immediately and reported to the IT department and department supervisor.

3.1 Training

Each State agency is responsible for ensuring that its employees are properly trained in accordance with this policy and any related internal agency policies and procedures. The Department of Information and Innovation will work with Agencies and The Summit: Center for State Employee Development to identify appropriate training opportunities.

3.2 Enforcement

Any employee found to have violated this policy may be subject to loss of privileges and/or disciplinary action, up to and including termination of employment.

4.0 Exceptions

With an understanding that each agency or department may have specific requirements, a waiver may be submitted to the Security Director (kris.rowley@state.vt.us) to request and exception. Each waiver will be evaluated on an individual basis.

Appendix A: General Password Construction and Guidelines

Passwords are used for various purposes within the State of Vermont agencies and departments as well as by vendors, contractors and other approved persons. Some of the more common uses include: user level accounts, Web accounts, e-mail accounts, screen saver protection and voicemail password. Since very few systems support one-time tokens, (i.e., dynamic passwords that are used only once), everyone should be aware of how to select strong passwords.

Do not use the same password for State of Vermont accounts as for other non-work related account access (e.g., personal Internet accounts, home computer access accounts, social networking accounts, etc.)

Poor, weak passwords have the following characteristics:

- The password contains less than eight characters
- The password is a word found in a dictionary (English or foreign)
- The password is a common usage word, such as:
    - Names of family, pets, friends, coworkers, fantasy characters, etc.
    - Computer terms and names, commands, sites, companies, hardware, software
    - The words "State of Vermont" or any derivation
    - Birthdays and other personal information such as addresses and phone numbers
    - Word or number patterns like aaabbb, qwerty, zyxwvuts, 123321, etc.
    - Any of the above spelled backwards
    - Any of the above preceded or followed by a digit (e.g., secre1, 1secret)

Strong passwords have the following characteristics:

- Contain both upper and lower case characters (e.g., a-z, A-Z)
- Have digits and punctuation characters as well as letters, (e.g., 0-9 , !#$%^&*(*)+~`-=\{}[]:";<>?@)
- Are at least eight alphanumeric characters long
- Are not a word in any language, slang, dialect, jargon, etc.

- Are not based on personal information, names of family, etc.
- Passwords should never be written down or stored online. Try to create passwords that can be easily remembered. One way to do this is create a password based on a song title, affirmation, or other phrase. For example, the phrase might be: "This May Be One Way To Remember" and the password could be: "Tmb1W>r~" or some other variation. *Note: Do not use either of these examples as passwords!*

Issuing Entity: Office of the Secretary, Agency of Administration

Approved: _____ **Date:** 2/25/10

Secretary of Administration